<u>AMENDMENTS TO THE CLAIMS</u>

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1.   (Previously Presented) A system that facilitates mitigation of outgoing spam, comprising:

a detection component employed by an outgoing message server that detects a potential spammer in connection with at least one outgoing message, the detection of a potential spammer being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account; and

an action component that upon receiving information from the detection component that the entity is a potential spammer, initiates at least one action that facilitates any one of confirming that the entity is a spammer, mitigating spamming by the entity, or increasing spammer cost, and a combination thereof.

2.   (Previously Presented) The system of claim 1, the outgoing message further comprising at least one of email message spam, instant message spam, whisper spam, or chat room spam.

3.   (Original) The system of claim 1 wherein the action initiated comprises at least one of:

shutting down the potential spammer's user account;

requiring any one of a HIP challenge and a computational challenge to be solved by the potential spammer and the potential spammer computer, respectively;

sending the potential spammer a legal notice regarding at least one violation of messaging service terms; and

manual inspection of at least a subset of outgoing messages generated by the potential spammer.

4.   (Previously Presented) The system of claim 1, wherein message volume monitoring comprises at least one of tracking or counting outgoing messages.

5.   (Previously Presented) The system of claim 1, wherein the detection is further based upon an outgoing message recipient count that is computed with each recipient counted only once.

6.   (Original) The system of claim 5, comprising keeping track of the maximum score per recipient.

7.   (Original) The system of claim 5, comprising using a pseudo-random function of recipients to estimate the recipient count, or related scores.

8.   (Previously Presented) The system of claim 1, wherein the detection is further based upon message rate monitoring comprising computing the volume of outgoing messages over a duration of time.

9.   (Previously Presented) The system of claim 8, wherein the duration of time comprises at least one of minutes, hours, days, weeks, months, or years.

10.   (Previously Presented) The system of claim 1, wherein the detection is further based upon message volume monitoring comprising a total volume of messages since activation of the entity's user account.

11.   (Original) The system of claim 1, wherein each recipient of an outgoing message constitutes one message.

12.   (Previously Presented) The system of claim 5, wherein the recipient count comprises one or more recipients listed in at least one of a to: field, a cc: field, or a bcc: field.

13.   (Previously Presented) The system of claim 1, wherein the detection component processes and analyzes the outgoing messages to determine at least one of whether the message is likely to be spam or whether the sender is a potential spammer.

14.   (Previously Presented) The system of claim 1, wherein the number of apparently legitimate messages is used as a bonus to offset other scores applied based upon one or more other indications of spam.

15.   (Original) The system of claim 14, wherein the number of apparently legitimate messages is estimated with a spam filter.

16.   (Previously Presented) The system of claim 14, wherein the bonus from the number of apparently legitimate messages is limited.

17.   (Previously Presented) The system of claim 1, wherein the number of non-deliverable messages is estimated at least in part from failures at message delivery time.

18.   (Original) The system of claim 1, wherein the number of non-deliverable messages is estimated at least in part from Non Delivery Receipts.

19.   (Original) The system of claim 18, wherein validity of the Non Delivery Receipts is checked.

20.   (Original) The system of claim 19, wherein validity of the Non Delivery Receipts is checked against a list of recipients of messages from the sender.

21.   (Original) The system of claim 20, wherein the list of recipients is a sample and the penalty of a Non Delivery Receipt is correspondingly increased.

22.   (Original) The system of claim 1, wherein the detection component computes scores assigned to the outgoing messages to determine a total score per sender and compares the total score per sender with at least one threshold level to ascertain whether the sender is a potential spammer.

23.   (Original) The system of claim 22, wherein threshold levels are adjustable per sender.

24.   (Previously Presented) The system of claim 1, wherein spam filtering comprises employing a filter trained to recognize at least one of non-spam like features or spam-like features in outgoing messages.

25.   (Original) The system of claim 1, wherein spam filtering is performed with a machine learning approach.

26.   (Original) The system of claim 1, wherein spam filtering comprises assigning a probability per outgoing message to indicate a likelihood that the message is any one of more spam-like or less spam-like.

27.   (Previously Presented) The system of claim 1, further comprising a scoring component that operates in connection with at least one of the spam filtering, total recipient count, unique recipient count, message volume monitoring or message rate monitoring.

28.   (Previously Presented) The system of claim 27, wherein the scoring component assigns a score per sender based at least in part upon at least one of volume of outgoing messages, rate of outgoing messages, recipient count, or message content.

29.   (Previously Presented) The system of claim 27, wherein the scoring component at least one of assigns or adds a constant value to one or more outgoing messages to mitigate spammers from manipulating spam filtering systems.

30.   (Original) The system of claim 27, wherein the scoring component assigns a selected value to outgoing messages identified as having at least one spam-like feature.

31.   (Original) The system of claim 30, wherein the at least one spam-like feature is a URL.

32.   (Original) The system of claim 30, wherein the at least one spam-like feature comprises contact information.

33.   (Previously Presented) The system of claim 32, wherein the contact information comprises a telephone number, the telephone number comprising at least one of an area code or a prefix to identify a geographic location associated with the message to thereby facilitate identifying the potential spammer.

34.   (Original) The system of claim 1, further comprising a user-based message generator component that generates outgoing messages addressed to one or more recipients based in part upon sender preferences.

35.   (Previously Presented) A method that facilitates mitigation of outgoing spam comprising:

detecting a potential spammer in connection with at least one outgoing message, the detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account;

receiving information from the detection component that the entity is a potential spammer; and

initiating at least one action that facilitates any one of confirming that the entity is a spammer, mitigating spamming by the entity, or increasing spammer cost.

36.   (Previously Presented) The method of claim 35, wherein the at least one outgoing message further comprises at least one of mail message spam, instant message spam, whisper spam, and chat room spam.

37.   (Previously Presented) The method of claim 35, further comprising monitoring outgoing messages per sender with respect to at least one of a volume of outgoing messages, a volume of recipients, or a rate of outgoing messages.

38.   (Previously Presented) The method of claim 35, wherein detecting a potential spammer comprises:

performing at least two of the following:

assigning a score per outgoing message based at least in part upon content of the message;

assigning a score per sender based at least in part upon outgoing message volume per sender;

assigning a score per sender based at least in part upon outgoing message rate per sender;

assigning a score per sender based at least in part upon a total recipient count per sender; or

assigning a score per sender based at least in part upon a unique recipient count per sender;

computing a total score per sender based upon two or more of the score per outgoing message, the score per sender based at least in part upon outgoing message volume per sender, the score per sender based at least in part upon outgoing message rate per sender, the score per sender based at least in part upon a total recipient count per sender, or the score per sender based at least in part upon a unique recipient count per sender; and

determining whether the sender is a potential spammer based at least in part upon the total score associated with the sender.

39.   (Original) The method of claim 38, wherein the total score exceeds a threshold level which thereby indicates that the respective sender is at least a potential spammer.

40.   (Original) The method of claim 35, further comprising tracking one or more recipients and associated outgoing messages addressed to the recipients to facilitate identifying one or more most spam-like messages received per sender.

41.   (Original) The method of claim 40, further comprising assigning one or more scores to the one or more most spam-like messages and aggregating the scores per sender to compute a total score per sender.

42.   (Original) The method of claim 35, wherein the at least one action comprises terminating the sender account.

43.   (Original) The method of claim 42, wherein the sender account is terminated when there is substantial certainty that the outgoing messages sent by a sender are spam.

44.   (Previously Presented) The method of claim 43, wherein substantial certainty that the outgoing messages are spam is determined in part by at least one of the following:

    at least a portion of the outgoing message comprises at least one of an exact
    match and a near match to known spam;

    at least a portion of the outgoing message comprises a phrase that a human has
    determined to be spam-like;

    a probability assigned by a spam filtering filter exceeds at least one threshold
    level; or

    a message sent for human inspection is determined to be spam.

45.   (Original) The method of claim 35, wherein the at least one action comprises temporarily suspending outgoing message delivery from the sender account.

46.   (Original) The method of claim 35, wherein the at least one action comprises requiring the sender account to resolve one or more challenges.

47.   (Original) The system of claim 44, wherein the account is volume limited per challenge until a determined number of challenges are solved, and is then rate limited thereafter.

48.   (Original) The system of claim 45, wherein the rate limit may be increased by solving additional challenges.

49.   (Original) The method of claim 46, wherein the one or more challenges comprise a computational challenge or a human interactive proof.

50.   (Original) The method of claim 46, wherein the one or more challenges are delivered as a pop up message.

51.   (Original) The method of claim 46, wherein the one or more challenges are delivered to the sender account *via* a message format similar to the sender's outgoing messages.

52.   (Original) The method of claim 46, wherein the one or more challenges are delivered to the sender account in response to feedback from a server that a shutdown of the account is approaching.

53.   (Original) The method of claim 35, wherein the at least one action comprises sending a legal notice that the sender is in violation of terms of service.

54.   (Previously Presented) The method of claim 53, comprising responding to the legal notice *via* at least one of providing an electronic signature or clicking on a link.

55.   (Original) The method of claim 53, wherein the legal notice is delivered *via* a pop-up message.

56.   (Original) The method of claim 35, wherein delivery of outgoing messages is temporarily suspended until a response to the action is received.

57.   (Original) The method of claim 35, wherein a minimum number of outgoing messages are permitted for delivery before a response to the action is received.

58.   (Original) The method of claim 35, further comprising estimating a total volume of recipients per sender to facilitate identifying a potential spammer.

59.   (Original) The method of claim 58, wherein estimating a total volume of distinct recipients per sender comprises:

computing a hash function per recipient to obtain a hash value per recipient;

setting a hash modulo value; and

adding the recipient to a list for message tracking when the recipient's hash value equals the hash modulo value to facilitate estimating a total volume of distinct recipients per sender.

60.   (Original) The method of claim 59, further comprising:

tracking worst-scoring messages each listed recipient receives per sender;

computing a total score of substantially all listed recipients' scores per sender; and

comparing the total score per sender with a threshold level associated with the sender to determine whether the sender is a potential spammer.

61.   (Previously Presented) A method that facilitates periodic validation of non-spammer like activity by a user account comprising:

monitoring the user account for at least one of a volume of outgoing messages, a volume of recipients in one or more outgoing messages, or a rate of outgoing messages;

requiring an owner of the user account to resolve one or more challenges after at least one of a number of outgoing messages sent from the user account exceeds a predetermined threshold or a number of recipients counted in one or more sent messages from the user account exceeds a predetermined threshold; and

suspending sending of subsequent outgoing messages from the user account until the one or more challenges are resolved.

62.   (Original) The method of claim 61, wherein each recipient listed in a message counts as an individual message.

63.   (Original) The method of claim 61, wherein the challenge is a computational challenge.

64.   (Original) The method of claim 61, wherein the challenge is a human interactive proof.

65.   (Previously Presented) A method of mitigating spam comprising:

        performing at least one economic analysis to determine sender outgoing message volume limit based at least in part on spammer behavior and legitimate user behavior; and

        limiting the sender outgoing message volume to at least one of:

            a maximum number per challenge resolved; or

            a maximum number per fee paid by a sender.

66.   (Previously Presented) The method of claim 65, wherein the challenge is at least one of a human interactive proof or a computational challenge.

67.   (Previously Presented) The method of claim 65, wherein the fee is any one of a user account set up fee, a monthly fee, a per-outgoing message fee, or a per number of outgoing messages fee.

68.   (Original) The method of claim 65, wherein the fee is limited to an amount that is low enough for legitimate users to willingly pay and high enough to mitigate sending spam messages.

69.   (Original) The method of claim 65, wherein a sender volume limit restricts a number of outgoing messages over a duration of time.

70.   (Previously Presented) A computer readable storage medium comprising the method of claim 1.

71.   (Previously Presented) A computer-readable storage medium having stored thereon the following computer executable components:

a detection component employed by an outgoing message server that detects a potential spammer in connection with at least one outgoing message, the outgoing message comprising at least one of e-mail message spam, instant message spam, whisper spam, or chat room spam, the detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account; and

an action component that upon receiving information from the detection component that the entity is a potential spammer, initiates at least one action that facilitates any one of confirming that the entity is a spammer, mitigating spamming by the entity, increasing spammer cost, or a combination thereof.

72.   (Previously Presented) A data packet adapted to be transmitted between two or more computer processes facilitating identify potential spammers, the data packet comprising:

information employed by an outgoing message server associated with detecting spam-like characteristics with at least one outgoing message, the outgoing message comprising at least one of instant message spam, whisper spam, and chat room spam, the detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account, wherein the information determines whether to initiate at least one action that facilitates any one of confirming that the entity is a spammer, mitigating spamming by the entity, or increasing spammer cost.

73.   (Previously Presented) A system that facilitates spam detection comprising:

a means employed by an outgoing message server for detecting a potential spammer in connection with at least one outgoing message, the outgoing message comprising at least one of e-mail message spam, instant message spam, whisper spam, and chat room spam, the

detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account or number of non-deliverable messages sent from the entity's user account;

        a means for receiving information from the detection component that the entity is a potential spammer; and

        a means for initiating at least one action that facilitates any one of confirming that the entity is a spammer, mitigating spamming by the entity, or increasing spammer cost.

      74.   (Previously Presented) A system that facilitates periodic validation of non-spammer like activity by a user account comprising:

        a means for monitoring a user account for at least one of a volume of outgoing messages, a volume of outgoing message recipients, or a rate of outgoing messages;

        a means for requiring an owner of the user account to resolve one or more challenges after at least one of a number of outgoing messages sent from the user account exceeds a predetermined threshold or a number of recipients counted in one or more sent messages from the user account exceeds a predetermined threshold; and

        a means for suspending sending of subsequent outgoing messages until the one or more challenges are resolved.

      75.   (Previously Presented) A system that facilitates mitigating spam comprising:

        a means for performing at least one economic analysis to determine sender outgoing message volume limit based at least in part on spammer behavior and legitimate user behavior; and

        a means for limiting the sender outgoing message volume to at least one of:

            a maximum number per challenge resolved; or and

            a maximum number per fee paid by a sender.